MITRE PRODUCT

State of the Art in Anomaly Detection and Reaction

An Update

February 24, 2000

Leonard J. LaPadula

This document has been approved for public dissemination; distribution is unlimited.

MITRE

**Center for Integrated Intelligence Systems
Bedford, Massachusetts**

Abstract

This supplement updates the author's views on trends in the market place and in government research and development based primarily on additional information gathered after the original report was published.

KEYWORDS: anomaly detection and reaction, state of the art, intrusion detection and reaction, vulnerability scanning, policy compliance scanning, network monitoring, host monitoring, anomaly response, intrusion response

Preface

This paper is a supplement to my 1999 report on the state of the art in anomaly detection and reaction (ADR) systems [1] and depends heavily on its companion paper, the ADR compendium [2]. Before addressing the main purpose of this supplement, I feel I owe it to the reader to say a few words about the use of the word "anomaly". I want also to note changes and additions made to the types of tools covered since the original report was published.

About the Use of the Word "Anomaly"

Unfortunately, as has been noted by several authors over the past few years, there is not yet a common vocabulary for talking about the technical area that encompasses intrusion detection, vulnerability scanning, security policy compliance monitoring, and related topics. When I started my 1999 report, I decided to use terminology that made sense to me, based on the usual meanings of words as described in modern dictionaries. It was this that gave rise to my use of the word "anomaly" to refer to anything out of the ordinary, normal, or expected in the configuration and operation of a network and the components within or attached to it[1]. This usage has *not* gained any noticeable acceptance in the past year. The community generally uses the word "anomaly" in a restricted technical sense to mean what I have called statistical deviation detection—that is, the word generally refers to deviant user behavior. In the face of overwhelming numbers of people using the word in that way, I must admit defeat and find another word. I have tried, but with no success to date. To backtrack to calling the entire set of "anomaly" tools "intrusion detection" tools is too egregious a misuse of the language for me to adopt that approach. Since I have not yet found an acceptable substitute, this supplement uses the terminology I adopted in the 1999 report; my apologies for any confusion I have caused.
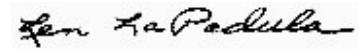
About the Types of Tools Available

Since the original report, I have changed the type "Analysis Engine" to "Analyzer", with the same definition as before. I have added the type "Decoy", defined as follows:

A decoy tool or system provides, simulates, or emulates a computer system or network system to provide a target for a cyber attacker, whether an insider or an outsider. Tools of this type would typically collect data about intrusive activity, providing alerts and reports, possibly collecting evidence to be used in legal action, and so forth.

---

[1] Please see the original report for a discussion of this area.

Finally, I have added the type "Network Scanner", with this definition:

A network scanner looks for evidence of network conditions that might provide an intruder or attacker an exploitable entrée into the network or the systems on the network.

January 25, 2000

State of the Art in Anomaly Detection and Reaction
An Update

Introduction

This paper is a supplement to the 1999 report on the state of the art in anomaly detection and reaction systems [1]. Although this supplement claims there are no major trends discernible since publication of the report, it should nevertheless have utility for anyone interested in the state of the art in anomaly detection and reaction as it is described in the 1999 report. There have been some noteworthy developments in the past year or so, including new commercial tools being released and new government research initiatives.

We first consider who the market leaders seem to be and take a look at mergers, acquisitions, and product transfers. We revisit commercial offerings and government research and development efforts. Based on these short reviews and other information gathered over the past year, we consider technical trends.

This supplement is organized as follows:

- Commercial Products: a look at the marketplace and a summary of commercial products based on an updated ADR Compendium [2]
- Research and Development: identification of some new initiatives
- Technical Trends: discussion of trends and commentary on what the state of affairs augurs for our military sponsors

Commercial Products

Market Leaders

The Hurwitz Group identified market leaders in its 1998 report on assessing risks and detecting intrusions [3]. It based its assessment on 1997 revenues; it also included two vendors (not specified in the report) who either were acquired or acquired another company, resulting in their having a viable product-distribution capability. Hurwitz Group identified Axent Technologies, Inc. and Internet Security Systems (ISS) as the top market leaders, with 1997 revenues of approximately $28 and $13 million respectively. The others ranged from $5m (Intrusion Detection, Inc.[2]) to about $1m (Network Associates, Inc.).

---

[2] Intrusion Detection, Inc. marketed the Kane Security Analyzer principally to the Wall Street market according to the Hurwitz Group report [1].

According to the report, the leaders in March 1998 were

- AXENT Technologies
- Internet Security Systems
- Intrusion Detection, Inc.
- Trusted Information Systems
- WheelGroup
- Veritas
- Network Associates, Inc.
- Others (Abirnet, Centrax, Netect, SAIC, and Trident Data Systems: $8 million collectively)

Through acquisitions, mergers, and product transfers, all of the "others" listed as well as TIS, WheelGroup, and Veritas have been absorbed by or have transferred their products to the other leaders or new companies. The apparent leaders today, listed alphabetically, are

- AXENT Technologies
- Cisco
- Internet Security Systems
- Network Associates, Inc.
- ODS Networks, Inc.
- PLATINUM technology

Acquisitions, Mergers, and Product Transfers

BindView Development Corporation acquired Netect, Inc. March 2, 1999; the Netective product became HackerShield. Subsequently, BindView released NOSAdmin for Windows NT (vulnerability scanner) in June 1999.

Cisco acquired WheelGroup about early 1998. WheelGroup was best known for its NetRanger product, which generated a good revenue stream for WheelGroup (Hurwitz Group estimated it had 5% of the market in 1997).

McAfee merged with Network General in 1997 to form Network Associates, Inc. (NAI). Network General had a CyberCop product, shipping since early March 1998, an intrusion detection technology that complemented the TIS Haystack Stalker risk assessment product line that Network Associates acquired in early 1998. NAI acquired Trusted Information Systems (TIS) sometime in early 1998. TIS, now a division of NAI, produced Stalker and ProxyStalker.

L-3 Network Security (Expert 3.0), formerly part of Trident Data Systems, is now part of L-3 Communications Corporation.

Veritas, through a 1997 merger with OpenVision, acquired a line of security products that included AXXiON-SecureMax, a risk assessment product. Early in 1998, Veritas sold its security products to PLATINUM Technology, which rebranded the Veritas product SecureMax as AutoSecure.

In September 1998, ODS Networks acquired the Computer Misuse and Detection System (CMDS) from Science Applications International Corporation (SAIC). The product is now referred to as the CMDS Enterprise system. In September 1999, ODS Networks assumed the ongoing development, marketing, sales, and support of the Kane Security Analyst vulnerability assessment tool and Kane Security Monitor intrusion detection system (both products of the small firm Intrusion Detection, Inc.) to complement its CMDS Enterprise system.

COMPAQ and Digital Equipment Corporation merged, effective June 11, 1998. The POLYCENTER family of products for Digital systems (system monitor, intrusion detector, security compliance scanner), which were produced before the merger (circa 1993/1994), are marketed by COMPAG, Digital Products and Services.

Abirnet was acquired by or became a subsidiary of MEMCO Software Ltd. MEMCO Software was acquired by PLATINUM Technology, March 29, 1999. PLATINUM Technology seems to have been acquired by or become a subsidiary of Computer Associates sometime since then.

AXENT acquired Internet Tools, Inc. (maker of ID-Trak), apparently sometime in 1999.

Figure 1 pictorially summarizes these acquisitions, mergers, and product transfers, leaving out the uncertain facts we mentioned above.
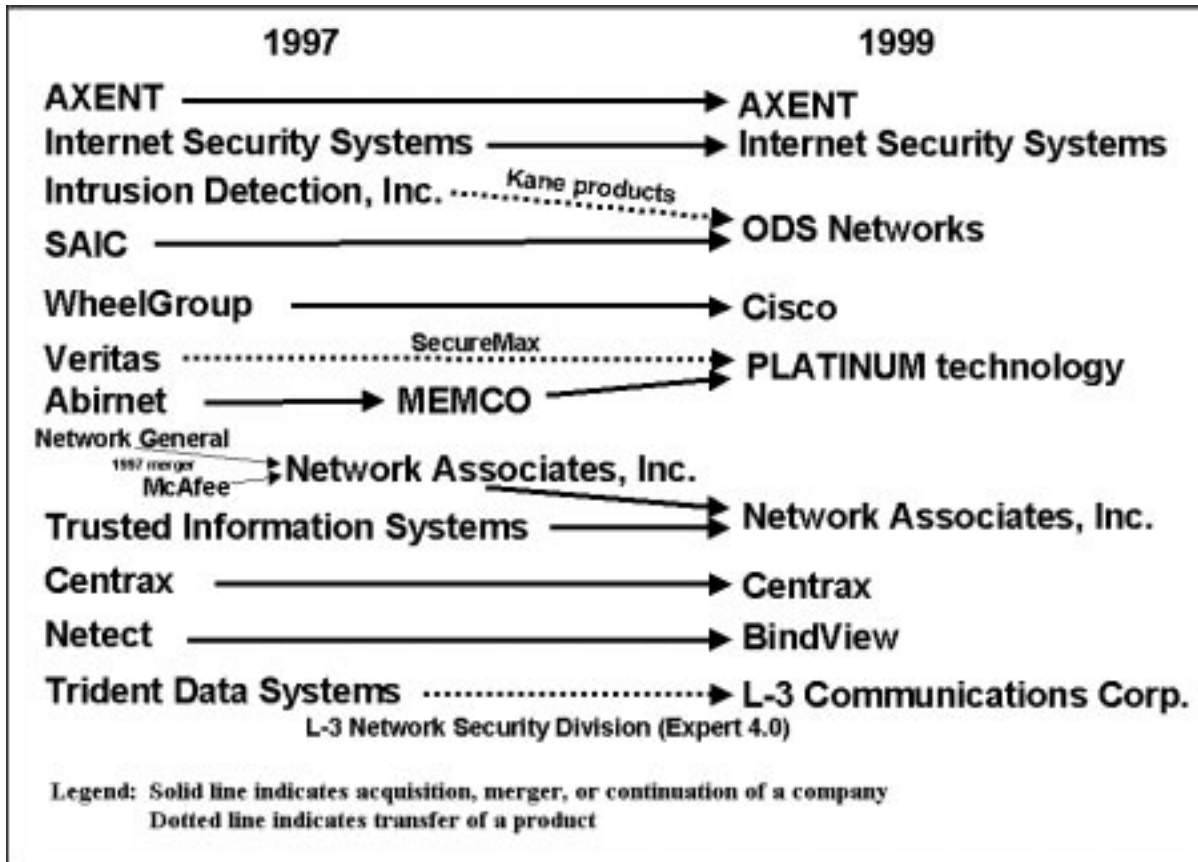

Figure 1. Acquisitions, Mergers, and Product Transfers

The 1999 state-of-the-art report suggested that a trend toward providing suites of integrated products might be developing in the commercial sector [1]. This was based on noticing that one or two "suite-like" products had become available. On the topic of "integration of tools into comprehensive ADR systems," the report stated that "rudimentary capabilities are beginning to show up in COTS products, typically as a bundled suite of previously independent tools by the same vendor; this is an area that GOTS products developed earlier than the commercial vendors and current government-funded efforts continue to lead in this area." It appeared that mergers and acquisitions would enable the trend toward integrated suites to expand and encompass more diverse products. Contrary to expectations, however, this aspect of the trend toward suites seems not to have developed.

Recently, PC Week Online reported that Network Associates, Inc. (NAI) would move[3] toward breaking up into five companies, with its software business splitting into four units: McAfee Inc., anti-virus sofware; PGP Security Inc., encryption, firewall and VPN software; Magic Solution Inc., help-desk software; and Sniffer Technologies Inc., network management tools [4]. According to the report, the security market did not develop the way NAI and others thought it would, that is, with suites dominating the market. Smaller companies that focused on particular technologies dominated NAI in their chosen technologies. Thus, it appears that the "trend" toward consolidation pictured in Figure 1 may not be a trend at all. While some vendors do offer closely related products that can interface to the vendor's own common, control or management software, it appears that the burden of integrating diverse types of tools into comprehensive ADR systems will continue to be borne by the government.

Research and Development

Since publication of the 1999 state-of-the-art report there have been new programs started by the government and we have become aware of a collection of efforts underway at Air Force Research Laboratory (AFRL), Rome Location. These projects have been described in the revised Compendium [2]. They are

- Air Force Enterprise Defense (AFED)
- Common Intrusion Detection Director System (CIDDS)
- Lighthouse
- Outpost
- Projects at Air Force Research Laboratory (AFRL), Rome Location

We briefly state the main thrust of each effort and comment on how it participates in defining the state of the art.

AFED **Thrust**: Move EPIC^2 concepts[4] closer to operational use.
Comment: This project appears to be significant for its attempt to satisfy user needs and preferences, adopting a pragmatic approach to implementing an idea that appeared promising theoretically.

---

[3] Sometime in the first quarter of calendar year 2000.

[4] EPIC^2 is fully described in the Compendium [2].

CIDDS	**Thrust**: Assimilate data from each of the CITS NMS/BIP tools[5] to realize hierarchical implementation of Air Force intrusion detection. **Comment**: This project appears to have pragmatic objectives similar to those of the AFED project while addressing an operational problem on the largest scale yet attempted anywhere; it is also significant, as is AFED, because it attempts to integrate the operations of diverse ADR tools.
Lighthouse	**Thrust**: The major part of this project is to develop prototypes based on usable concepts from research and move them into the functional and operational infrastructure of the Air Force; it also is addressing testing strategies and the state of the practice[6]. **Comment**: This project appears to provide a needed venue for enabling technology insertion and technology management in the ADR area.
Outpost	**Thrust**: Provide a technical infrastructure for the Lighthouse Project on which sensors, analyzers, reporters, and directors can interoperate to provide situation awareness; reaction, remediation, and reconstitution capabilities; and decision support. **Comment**: Besides obvious similarities in objectives to AFED and CIDDS, this project's technological innovations in infrastructure appear to be significant. The infrastructure provides host-based agents that can accept probes from a central manager, run the probes, and report the results to the manager. This promises the capability to incorporate diverse products from different vendors into a single ADR management system.

---

[5]   For a description of CITS NMS/BIP and the security tools it provides, see Reference 6, report on ADR tools for the tactical environment.

[6]   See the Reference 5, report of Software Engineering Institute.

Projects at AFRL **Thrust**: Encourage research and development in numerous areas related to information assurance with a focus on anomaly detection and reaction.

Comment: This group of small research efforts represents the only government initiative we are aware of that addresses the area of damage assessment and recovery.

Technical Trends

One can sometimes identify trends based on quantitative observations. In the ADR area it is tempting to count types of products, how many products of what type were released in a given year, and so forth. We do not have enough information to support such quantitative studies. However, we did count commercial tools by type using the information in the Compendium [2]. The appendix to this paper has a listing of tools, showing vendor, type, and estimated release date, and the count of tools by type. From the compiled data, we can only conclude that there are no new trends discernible[7]. One can interpret this observation to mean that the status quo prevails, with all of its attendant problems, as described in our 1999 report [1]. However, this idea needs qualification, which we provide by characterizing technical trends based on non-quantitative observations.

Two new types of tools showed up in the commercial category in 1999: a network scanner and a decoy; see the Compendium for details on Anti-Sniff and CyberCop Sting [2]. The point of interest here is that the variety of tools under the general category of ADR has continued to increase.

There is a trend both by commercial vendors and in research efforts toward developing and investigating host-based intrusion detection, while network-based monitoring has fallen out of favor with some. Nevertheless, new products in the latter category continue to be released by the vendors. Thus, it appears that there has been a broadening rather than a shift in approach. However, the recent state-of-the-practice report by SEI identifies trends in networking that may mean that network-based monitoring will have a decreasing role in the next few years. Commenting on the increasing bandwidth available, migration to switched as opposed to broadcast local network segments, and the growing use of virtual private networks and encrypted tunnels, SEI concluded that "As a consequence, network-based ID systems will have decreasing applicability and will have to be replaced by alternative approaches." [5]

---

[7] Nor were any trends along these lines reported in the recent state-of-the-practice report by Software Engineering Institute [4].

The trend toward automatic updates via the Internet as new vulnerabilities and attacks are codified appears to be continuing among vendors of vulnerability scanners and intrusion detectors.

In the 1999 report, we identified a trend toward suites of products, within a vendor's family of closely related products, whose outputs can be integrated. Although one new offering during the past nine months appears to follow this pattern, one is hard pressed to continue claiming that this is a trend. New specific products are more likely to be released, it seems, than complete suites of related products, sometimes with a packaged collection that incorporates previously released products being offered later.

There is a growing realization that preventive measures that deter or disable attack capability can be more cost-effective than intrusion monitoring since, in general, a detected attack may have already caused damage while a prevented attack cannot cause damage. One author has identified specific circumstances when they may be more cost-effective: (1) when only the preventive measures can be afforded and (2) when network administrators are just beginning to pay attention to the intrusion problem and have not yet formulated policies and procedures [3]. These are ideas that this author strongly endorses.

It is still the case, as it has been for several years, that commercial vendors and military researchers/developers work on different aspects of the general anomaly management problem. Vendors develop tools that tend to target fairly specific markets. The outstanding example is the fact that the products of the vendor with the second largest revenues, Intrusion Detection, Inc., as reported in the Hurwitz Group report, are deployed almost exclusively on Wall Street [3]. The military continues to work on the broader aspects of the problem, focusing on decision support for the commander. This leads them to efforts like EPIC[2] and its follow-on AFED, and sponsored projects like Lighthouse. These ideas invite the question: Is this difference between commercial offerings and military needs widening or just persistent in the ADR area?

The Information Assurance Product Area Directorate at ESC developed a special contractual relationship with L-3 Network Security to add functionality to its Expert 3.0 risk management product, resulting in Expert 4.1. This effort has increased the utility of the tool for the Air Force and has resulted in a more capable product that L-3 Network Security can sell commercially. This kind of arrangement may provide a model for government-commercial partnering that could improve the utility of ADR products. Aside from this, however, we are aware of no other specific initiatives to directly influence vendor products.

One of the problems that arises out of this situation is that the military is not equipped to develop operational systems effectively. It needs the expertise and production facilities that the commercial vendors have. At the same time, though, the vendors appear to need incentives to produce the systems the military needs. Without an ongoing dialog, the current

situation may continue indefinitely with very little of the research and development done by or for the military ever getting fielded in a usable operational form with high utility.

Since the publication of the first version[8] of its technical framework document, the Information Assurance Technical Framework (IATF) Forum appears to have achieved a leadership position in bringing together the producers and consumers of information assurance technologies. With representatives from all the military departments, a number of other government agencies, and many vendors attending the monthly meetings to discuss selected information assurance topics and to generally exchange ideas and information, the Forum appears to provide the best venue available to date in which the military can influence vendors to provide the ADR products it needs.

The latest version of the technical framework explicitly identifies commercial vendors and the commercial research community among the members of its intended audience:

> "The Framework will be used by commercial product and service providers to get insight into the needs of our customers. The high level security requirements are captured and presented in each of the customer requirement categories as well as in the Characterization of the Customer Community chapter. Customers will be able to see that their problems are being addressed and industry will get an indication of the current and future markets for security products and services.

> "The Framework will highlight future IA technology research areas. The identification of gaps highlighted in the Framework will be available to both the internal National Security Agency and commercial research communities. These gaps will show where new technologies or new techniques are needed to further strengthen the security of the Defense Information Infrastructure (DII) and the National Information Infrastructure (NII). The research areas will also be tied to current and future customer requirements. This linkage will increase the probability that the resulting solutions will be used."

At present, however, the IATF does not identify customer needs in the area of ADR systems, except in very high level terms. The section[9] intended to give an overview of the detect and respond supporting infrastructure is yet to be developed. Although there is some assessment of the state of the art in the ADR area, it is currently based on somewhat dated reports[10].

---

[8] *Network Security Framework*, Version 1.0, May 28, 1998.

[9] Section 2.7.2 Detect and Respond Supporting Infrastructure Overview.

[10] *Intrusion Detection Fly-Off: Implications for the United States Navy*, MITRE Technical Report 97W0000096 and the *National Info-Sec Technical Baseline: Intrusion Detection and Response*, Lawrence Livermore National Laboratory.

Encouraging signs in a related area come from the orientation of the EPIC2 and the new AFED and CIDDS projects, each of which has among its goals to provide the commander with better decision-support capability. These efforts augur well for increased understanding of the needs of the operations-oriented decision makers on the part of the researchers within the government.

During the last year there has been project funding in the Air Force for investigating damage assessment and recovery capabilities, a hitherto neglected area in this technology arena: see the Damage Assessment and Recovery group in the AFRL Projects listing in the ADR Compendium [5]. While this does not constitute a trend, it is a beginning in addressing an important area.

The work on forensic analysis in projects at MITRE and AFRL does constitute a trend that started around fiscal year 1998 with an Air Force MOIE project at MITRE. In 1999, at least one vendor claimed to provide forensically useful information.

Finally, one should not overlook the very significant standards work that has been done by the Common Vulnerabilities and Exposures (CVE) effort started by The MITRE Corporation in 1999. The CVE is a list of standardized names for vulnerabilities and other information security exposures. The CVE dictionary will make it easier to share data across separate vulnerability databases and security tools [7]. The fact that the CVE is getting support from many vendors and other interests suggests that other standardization goals that could be approached in the manner of the CVE might also succeed.

List of References

1. LaPadula, L. J., May 1999, *State of the Art in Anomaly Detection and Reaction*, MP 99B000020, approved for public dissemination, The MITRE Corporation, Bedford, Massachusetts.

2. LaPadula, L. J., January 2000, *Compendium of Anomaly Detection and Reaction Tools and Projects: Version 2*, MP 99B0000018R1, approval for public dissemination expected by April 14, 2000, The MITRE Corporation, Bedford, Massachusetts.

3. Hurwitz Group, Inc., March 1998, *Information Security: Assessing Risks and Detecting Intrusions*, White Paper viewable at Summit OnLine on December 27, 1999.

4. Kerstetter, J., January 14, 2000, *Network Associates calls it quits on suite plan*, PC Week Online, http://www.zdnet.com/pcweek/.

5. Allen, J., A. Christie, W. Fifthen, J. McHugh, J. Pickel, E. Stoner, December 1999, *State of the Practice of Intrusion Detection Technologies*, Technical Report CMU/SEI-99-TR-028, ESC-99-028, Carnegie Mellon, Software Engineering Institute, Pittsburgh, Pennsylvania.

6. LaPadula, L. J., August 1999, *Anomaly Detection and Reaction Capabilities for the Air Force Deployed Tactical Data Networking Infrastructures*, MTR 99B0000037, The MITRE Corporation, Bedford, Massachusetts.

7. CVE Editorial Board, January 1999, http://cve.mitre.org.

Appendix

Summary of COTS ADR Products

This information was compiled on December 30, 1999 from the ADR Compendium [5].

Name of Tool	Type	Released	Vendor
AntiSniff, Version 1.0 (July, 1999)	Network Scanner	July 1999	LOpht
AutoSecure Access Control (for Windows NT or for UNIX)	System Monitor for Access Control	≤ 1998	PLATINUM
AutoSecure Policy Compliance Manager	Security Compliance Scanner	≤ 1998	PLATINUM
BlackICE Pro	System Monitor	May 10, 1999	Network ICE
Computer Misuse Detection System (CMDS™)	System Monitor	≤ 1998	ODS Networks
CyberCop Monitor	System Monitor	1999	Network Associates
CyberCop Scanner, Version 2.5	Vulnerability Scanner	≤ 1998	Network Associates
CyberCop Server	System Monitor	1999	Network Associates
CyberCop Sting	Decoy	late 1999	Network Associates
Database Scanner 1.0	Vulnerability Scanner	≤ 1998	Internet Security Systems
Dragon Intrusion Detection System, Version 3.2	Network Monitor	August 20, 1999	Network Security Wizards
Enterprise Security Manager	Security Compliance Scanner	≤ 1998	AXENT
eNTrax Security Suite	System Monitor Vulnerability Scanner	≤ 1998	Centrax
Expert 3.0	Network Mapper Vulnerability Scanner Risk Analyst	≤ 1998	L-3 Network Security
HackerShield	Vulnerability Scanner	≤ 1998	BindView

Name of Tool	Type	Released	Vendor
ICEcap	Anomaly Detection and Reaction Director	1999	Network ICE
ID-Trak	Network Monitor	≤ 1998	AXENT (by acquisition of Internet Tools, Inc.)
Internet Scanner	Vulnerability Scanner	≤ 1998	Internet Security Systems
Intruder Alert	System Monitor Network Monitor with NetProwler Add-In	≤ 1998	AXENT
IP-Watcher	Network Monitor	≤ 1998	En Garde Systems
IRIS (INTOUCH Remote Interactive Supervisor)	Anomaly Detection Support Tool	≤ 1998	Touch Technologies
Kane Security Analyst for Novell	Vulnerability Scanner	≤ 1998	ODS Networks
Kane Security Analyst for Windows NT	Vulnerability Scanner	≤ 1998	ODS Networks
Kane Security Monitor for Windows NT	Infraction Scanner	≤ 1998	ODS Networks
NetBoy Suite of Software	Suite of Monitors	≤ 1998	NDG Software
NetProwler	Network Monitor	≤ 1998	AXENT
NetRanger	Network Monitor	≤ 1998	Cisco
NetRecon, Version 2.0	Vulnerability Scanner	≤ 1998	AXENT
NetSonar	Vulnerability Scanner	≤ 1998	Cisco
Network Flight Recorder, Version 2.0.2 (Commercial)	Anomaly Detection Support Tool	1999 (commercial version)	Network Flight Recorder
NOSadmin for Windows NT, Version 6.1	Vulnerability Scanner	June 1999	BindView
POLYCENTER Security Compliance Managers	Security Compliance Scanner	≤ 1997	COMPAQ, DIGITAL Products and Services

Name of Tool	Type	Released	Vendor
POLYCENTER Security Intrusion Detector for Digital UNIX, Version 1.2A	System Monitor	≤ 1997	COMPAQ, DIGITAL Products and Services
POLYCENTER Security Intrusion Detector for OpenVMS VAX and OpenVMS Alpha, Version 1.2a	System Monitor	≤ 1997	COMPAQ, DIGITAL Products and Services
POLYCENTER Security Reporting Facility (SRF)	ADR Director	≤ 1997	COMPAQ, DIGITAL Products and Services
PréCis 3.0	Audit Management Toolkit	≤ 1998	Litton PRC
ProxyStalker 1.0	System Monitor	≤ 1998	Network Associates, Inc., Trusted Information Systems Division
RealSecure™ 3.1	Network Monitor Infraction Scanner	≤ 1998	Internet Security Systems
SAFEsuite Decisions 1.0	ADR Director	≤ 1998	Internet Security Systems
SecureNet Pro	Network Monitor	1997	MimeStar
Security Configuration Manager for Windows NT 4	Security Compliance Scanner	≤ 1998	Microsoft
SeNTry – Enterprise Event Manager	System Monitor	≤ 1998	Mission Critical Software
SessionWall-3, Version 4.0	Network Monitor	February 9, 1999	PLATINUM
SFProtect - Enterprise Edition	Vulnerability Scanner Security Compliance Scanner	August 1999	Hewlett Packard
SilentRunner	unknown (vendor calls it a *Discovery, Visualization, and Analysis System*)	≤ 1999	Raytheon

Name of Tool	Type	Released	Vendor
Stake Out™ I.D.	Network Monitor	≤ 1998	Harris Communications
Stalker, Version 2.1	System Monitor	≤ 1998	Network Associates, Inc., Trusted Information Systems Division
System Scanner 1.0	Vulnerability Scanner Infraction Scanner	≤ 1998	Internet Security Systems

The next table groups tools by type, with the groups ordered by count. Dates for the release of the tools are estimated since release dates were not included in the first version of the Compendium, whence this data derives. Thus, the timeframe "≤ 1998" means the tool was released sometime before or during 1998-some of the tools may have been released as early as 1992 or so, for example, the POLYCENTER tools. Ten of the tools, however, were released sometime in 1999. The types shown in italics are special types not recognized in the ADR Compendium.

Type	Count	Timeframe
System Monitor	13	≤ 1997 (2) to ≤ 1998 (8) to 1999 (3)
Vulnerability Scanner	12	≤ 1998 (10) to 1999 (2)
Network Monitor	10	1997 (1) to ≤ 1998 (7) to 1999 (2)
Security Compliance Scanner	5	≤ 1997 (1) to ≤ 1998 (3) to 1999 (1)
ADR Director	3	≤ 1997 (1) to ≤ 1998 (1) to 1999 (1)
ADR Support Tool	2	≤ 1998 (1) to 1999 (1)
Infraction Scanner	2	≤ 1998
Analyzer	1	≤ 1998
Decoy	1	late 1999
Network Scanner	1	July 1999
Suite of Monitors	1	≤ 1998
Discovery, Visualization, and Analysis System	1	≤ 1999